Position Requirements Document Cover Sheet	Position Number: 12839

Classification: Interdisciplinary, NH-****-IV   **Opt:** Computer Engineer, 0854; CL: 435A
Local Title: Info Assurance Program Manager (IAPM)   **Opt:** Computer Scientist, 1550; CL: 435B
Employing Office Location: Orlando, FL
Duty Station: Orlando, FL

Org Info: **Agency:**   Assistant Secretary of the Army (Acquisition, Logistics and Technology) ASA(ALT)
     1st Div: Program Executive Office, Simulation, Training and Instrumentation (PEO STRI)
     2nd Div: Corporate Information Office
     3rd Div:
     4th Div:

Supervisor's Certification: I certify that this is an accurate statement of the major duties and responsibilities of this position and its organizational relationships, and that the position is necessary to carry out government functions for which I am responsible. This certification is made with the knowledge that this information is to be used for statutory purposes relating to appointment and payment of public funds, and that false or misleading statements may constitute violations of such statutes or their implementing regulations.
Immediate Supervisor: James H. McBrayer

Title: Chief Information Officer

Signature: _____/s/_____   **Date:**   16 April03

Higher Supervisor or Manager: _____

Title: _____

Signature: _____   **Date:** _____

Classification/Job Grading Certification: I certify that this position has been classified IAW Acquisition Workforce Personnel Demonstration Project broadbanding criteria.

Classification Official: Stephen M. Seay, BG

Title: Program Executive Officer

Signature: _____/s/_____   **Date:**   18 April 2003

FLSA:	Exempt	**BUS Code:**	7777 CL: 435A/B (see above)
Drug Test:	Yes	**Emergency Ess:**	
Key Position:		**OPM Functions Code:**	13
Sensitivity:	CS	**Status:**	Competitive
Reason for Submission:	New	**Subject to IA:**	No
Previous PD Number:		**Mobilization:**	
Envir. Diff:		**Career Prg ID:**	
Acq Posn Category:	R	**CAPL Number:**	
Acq Career Level:	3	**Acq Posn Type:**	1
Acq Special Asgmt:		**Acq Prog Ind:**	
Career Spec – Primary:		**Career Spec – Sec:**	
Cont Job Site:		**Mobility:**	

Financial Disclosure: [ ] Public Financial   [X] Confidential Financial
[ ] Supervisor   [ ] Manager   [X] Neither
Citation 1: USOPM PCS for Computer Engineering Series, GS-0854 TS-83 January 1988
Citation 2: USOPM PCS for Computer Science Series, GS-1550 TS-83 January 1988
Citation 3: AWF, PDP, BLD, Federal Register, Volume 64, Jan 99

<mark>**Top Secret Clearance w/SCI required**</mark>

Acquisition Workforce Demo Project
Position Requirements Document

I.   Organization information:

Position is located in the Corporate Information Office, Program Executive Office, Simulation, Training and Instrumentation (PEO STRI).

II. Position information:

Interdisciplinary, NH-****-IV.
    Opt: Computer Engineer, 0854
    Opt: Computer Scientist, 1550

III. Duties:

Serves as the Information Assurance Program Manager (IAPM) for PEO STRI. Serves as the PEO's single point of contact for Information Assurance matters associated with all acquisition programs in all phases of the life cycle (development through post deployment support).

Works with National Security Agency (NSA) to specify and design security products and guarding solutions to allow simulation and training systems to operate with tactical C4I and other systems that may operate at TS/SCI levels. These security products and guarding solutions will be integrated with simulation and training systems to provide high levels of confidence that classified information is not inadvertently transferred to the unclassified simulation systems.

The IAPM is the PEO's advisor as to the readiness of the complex simulation and training systems for accreditation and eventual materiel release. The IAPM serves as the PEO's authoritative representative for the review and accreditation of complex systems IAW the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). Authoritatively represents the Designated Approving Authority (DAA) (PEO/DPEO) at Certification Requirement Reviews (CRRs) and other critical meetings. Provides oversight to an in-house contractor workforce consisting of several personnel who assist in developing DITSCAP certification packages.

As the PEO's information assurance expert and manager, manages a program to ensure security of critical, state-of-the-art training systems, and advises the PEO, DPEO, Directorates and Program

Managers on all matters pertaining to information assurance. Oversees approximately 7 Information Assurance Managers (IAMs) and approximately 100 Information Assurance Security Officers (IASOs) who are responsible for information assurance on several hundred state-of-the-art training systems and other products developed by PEO STRI.

Interfaces on a regular basis with DA representatives to develop and influence Army policy and procedures in the area of Information Assurance.

Monitors the Army Contractor Automatic Verification System (ACAVS). Develops and manages policy, procedures and technical guidance for the security design, development and test efforts necessary for the accreditation and certification to include working within teams consisting of industry software architects, engineers and programmers.

Manages the organization's Information Assurance and has responsibility for assuring threat recognition, risk mitigation and security border identification.

Provides the system engineering discipline necessary to ensure proper design, implementation and integration of security features into the overall simulation/training system architecture and design. Integrates information assurance practices and procedures across all PMs and other Core Business Units.

Develops and promulgates the overall information assurance operating policies and procedures for PEO STRI. Coordinates with Senior Leadership for enforcing compliance with DA certification requirements. Plans, develops, implements and manages the Information Assurance Program; manages schedule and contract support services. Develops certification and accreditation processes to be followed by all PEO STRI's acquisition programs; coordinates and promulgates policy and procedures for the Information Assurance Program.

Ensures that system architectures incorporate state-of-the-art Cross-Domain Solutions (CDS), Firewalls, etc., that require connectivity to Secret Internet Protocol Router Network (SIPRNET) and Joint Worldwide Intelligence Communication System (JWICS). Ensures compliance with Government and appropriate industry standards and, in the absence of standards, represents the organizations in specific negotiations and specific planning efforts to correct deficiencies or revise or develop standards.

Develops, maintains and leads relationships with internal and external Information Assurance community to include senior DOD civilian and industry architects, engineers and Project/Program Managers.

Serves as PEO STRI's single point of contact to Department of Army CIO, National Security Agency (NSA) and the Top Secret and Below Interoperability (TSABI) organization.

Develops and implements the PEO STRI Information Assurance Vulnerability Alerts (IAVAs) policy to ensure compliance of PEO STRI developed and fielded systems. Reports compliance to the Department of Army and tracks internal Information Assurance metrics of the PMs and Directorates.

Keeps abreast of emerging information systems concepts, methods and techniques, which can potentially impact the security architectures.

Critical Acquisition Position
     "This is a Critical Acquisition Position. Unless specifically waived by the appropriate Army official, (i.e., the Director of Acquisition Career Management, the Army Acquisition Executive, or the Secretary of the Army) or if the employee is "grandfathered" under 10 U.S.C. 1736(c)(1), the following are statutorily mandated requirements (Reference: 10 U.S.C. 1733 and 1737):

     (1) Selectee must be a member of an Acquisition Corps at the time of appointment.

     (2) Selectee must execute, as a condition of appointment, a written agreement to remain in Federal service in this position for at least three years. In signing such agreement, the employee does not forfeit any terms or conditions of employment."

Must be able to obtain and maintain a Top Secret/Sensitive Compartmented Information (TS/SCI) clearance.

KNOWLEDGE, SKILLS, AND ABILITIES (KSAS) FOR QUALIFICATION PURPOSES

Professional knowledge of systems engineering principles, with special emphasis on computer software and hardware security architectures, Information Assurance, Cross-Domain Solutions (CDS), Firewalls, and related skills

Knowledge of the development and integration of state-of-the-art engineering concepts within modeling and simulation systems

Knowledge of Multi-Level Security development and approval process

Expertise in Information Assurance regulations, policies and standards

Expertise in Certification and Accreditation process and procedures

Experience with security measures required when linking Tactical C4I systems with simulations across the Live, Constructive and Virtual domains

Ability to communicate orally and in writing and to serve as a spokesman for the organization with senior executives and General Officers

Knowledge of the SIPRNET and JWICS connection process for simulation systems

Expertise in the Information Assurance Vulnerability Alerts (IAVAs) compliance process

Ability to development and implement Information Assurance Policies and Procedures

Ability to represent and serve as a spokesman for the organization with senior executives and General Officers at the National Security Agency, DA HQ, CIO and elsewhere